Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/AU05/000317

International filing date: 04 March 2005 (04.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: AU
Number: 2004901143
Filing date: 05 March 2004 (05.03.2004)

Date of receipt at the International Bureau: 19 April 2005 (19.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/AU2005/000317

Australian Government

Patent Office
Canberra

I, JANENE PEISKER, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2004901143 for a patent by SECURE SYSTEMS LIMITED as filed on 05 March 2004.

WITNESS my hand this
Eleventh day of April 2005

JANENE PEISKER
TEAM LEADER EXAMINATION
SUPPORT AND SALES

P/00/009 28/5/91
Regulation 3.2

ORIGINAL

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION

Invention Title: "Partition Access Control System and Method for Computers"

The invention is described in the following statement:

"Partition Access Control System and Method for Computers"

Field of the Invention

The present invention relates to a partition access control system and method for computers that has particular utility for controlling user access to a data store on a computer system.

Throughout the specification, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Background Art

The following discussion of the background art is intended to facilitate an understanding of the present invention only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was part of the common general knowledge as at the priority date of the application.

With widespread developments in computer networking technology and computer use generally, the security of computer systems and especially the accessing of data on storage media by such systems, has become of paramount importance to ward off unauthorised access of users and programs such as viruses, worms and other types of malware alike.

As disclosed in patent specification WO 03/003242, which is incorporated herein by reference, the applicant proposed a system and method for securing data and information stores in computer systems involving the use of a discrete security device interposed at some position along the data access channel between the host central processing unit (CPU) and the mass data storage media of the particular computer system being secured.

As described in the applicant's subsequent International Patent Application PCT/AU2004/000210, which is also incorporated herein by reference, this security device could not only be embodied in the form of an external device to the motherboard and hard disk drive, but also integrated into the bus bridge circuit provided on the motherboard at the CPU bus end of the computer system, communicating with the data access channel, or a bus bridge circuit provided in the hard disk drive itself at the mass storage media end of the data access channel.

As described in the aforementioned patent specifications, the system administrator for the security device had the facility to set data access permissions of various partitions provided on the mass storage media of the computer system for each permitted user of the computer system requiring access to such. In most cases, this would be every authorised user of the computer system. These data access permissions included, amongst others, read only access, write only access or read and write access to a specific partition. Accordingly, the system administrator could change the data access permissions for a particular user, and if desired, create different user profiles for the same user.

Thus, if a particular user was required to have one particular profile specifying data access permissions for different partitions when not connected to the Internet, and another profile preventing write access to certain key partitions when connected to the Internet that the user would otherwise normally have write access to, the administrator could created two separate profiles for that user, albeit under different user names. These different user names would have discrete password authentication for the particular user to adopt, but could be alternated between by the user depending upon the user's Internet connectivity requirements.

However, as described in the aforementioned patent specifications, in order to ensure the integrity of the computer system during the authentication process, the security device was designed to only authenticate users and assign access

profiles at start up of the computer system only, before the operating system of the computer system was loaded. The reason of this was that if the user was permitted to switch profiles during normal computer operation, this would significantly undermine the security provided by the security device, as well as create operating system dependencies, which as previously discussed, is highly undesirable.

Notwithstanding the need to maintain the integrity of the protection regime provided by the security device, if a user was operating the computer system under a first profile when not connected to the Internet, and then desired to connect to the Internet, it would be necessary for that user to cease their working session, shut down the operating system and restart the computer. The user would then be able to proceed through the authentication process again and adopt another user profile appropriate for connecting to the Internet.

Obviously, such a process proves to be quite inconvenient to a user of the system and significantly detract from the efficiency of operator use of the computer system.

An example of the process is described below with reference to Table 1:

User: 1	Profile: 1	Disk Access	C: Read/Write
			D: Read Only
			E: Read/Write
User: 1	Profile: 2	Disk Access	C: Read/Write
			D: Read/Write
			F: Read/Write
User: 1	Profile: 3	Disk Access	C: Read/Write
			G: Read Only
User: 2	Profile: 1	Disk Access	C: Read/Write
			H: Read/Write

Table 1

In this example, at start-up user 1 may authenticate using any of the three profiles set by the administrator to assign different access rights to the partitions for which the user is authorised to access. This prevents data from being written to partitions which are not selectable or are set as read only. To gain access to different partitions, user 1 must restart the computer and complete the authentication process using one of their remaining profiles. User 1 cannot authenticate as user 2, and so in this example, user 1 never can access the H partition.

As can be seen from the above example, it would of great advantage if user 1 could change its user profile without having to log off, restart and authenticate with a new user profile, each time it wished, or was required, to change its data access permissions when performing a new task which may compromise the integrity of the stored data from a security perspective.

Disclosure of the Invention

It is an object of the invention to provide for the improved control of users with respect to accessing data stored on a computer system.

In accordance with a first aspect of the present invention, there is provided a control system for controlling the access of users to data stored on a data store of a computer system, the data store being formatted to store data in a plurality of partitions, comprising:

authentication means to authenticate users permitted to access data stored in the data store;

database means to store the data access profile of each user permitted to access said data stored in the data store;

the data access profile including:

- a user name and password for each permitted user,

- the partitions of said data store to which the user is permitted access, and
- a permission state for each said partition to which the user is permitted access;

said permission state being one of a plurality of different read or write data access permissions, each data access permission providing a different degree of data access to data stored within a said partition, ranging from a low or no permission to read or write data from or to said partition, to a high or total permission to read or write data from or to said partition;

profile setting means for setting a master data access profile and a current data access profile for each permitted user in said database means; and

editing means for editing said current data access profile within parameters determined by said master data access profile.

Preferably, the control system includes access setting means to set access for a permitted user to said editing means, whereby when access is not set, the permitted user is denied access to said editing means, and when access is set, the permitted user is permitted access to said editing means.

Preferably, said editing means is accessible to a permitted user that is set access thereto during normal operation of the computer system by said permitted user, after loading of the operating system thereof.

Preferably, said profile setting means is operable to set said master data access profile and said current access profile prior to loading of the operating system of the computer system.

In accordance with a second aspect of the invention, there is provided a method for controlling the access of users to data stored on a data store of a computer system, the data store being formatted to store data in a plurality of partitions, the method comprising:

authenticating a user to only allow permitted users to access data in the data store;

storing the data access profile of each user permitted to access the data stored in the data store;

the data access profile including:

- a user name and password for each permitted user,
- the partitions of the data store to which the user is permitted access, and
- a permission state for each said partition to which the user is permitted access;

the permission state being one of a plurality of different read or write data access permissions, each data access permission providing a different degree of data access to data stored within a said partition, ranging from a low or no permission for reading or writing data from or to said partition, to a high or total permission for reading or writing data from or to said partition;

setting a master data access profile and a current data access profile for each permitted user; and

editing the current data access profile within parameters determined by the master data access profile;

wherein the determined parameters permit changing a data access permission for a partition to the same or lower degree than the data access permission set for a permitted user in the master data access profile thereof, and denying change of a data access permission to a higher degree than the data access permission set for the permitted user in the master data access profile thereof.

Brief Description of the Drawings

The accompanying drawings, which are referred to in the subsequent description of the Best Mode for Carrying Out the Invention, are briefly described as follows:-

Figure 1 is a block diagram showing the software system structure of the partition access control utility (PACU) with respect to the security device (SDV) for protecting the data store connected to the computer system, in accordance with the first embodiment of the invention;

Figure 2 is a block diagram of the logical structure of the PACU application and its interface with the SDV as described in the first embodiment;

Figure 3 is a depiction of the main screen displayed by the graphical user interface (GUI) showing some of the partitions provided on the data store of the computer system and the data access permissions available thereto for a particular user of the computer system to set for prescribed partition access control;

Figure 4 is a flow diagram showing the initialisation process for a computer system incorporating the SDV and the PACU application;

Figure 5 is a display panel displayed by the GUI for a super user to access the computer system and initialise user profiles therefor;

Figure 6 is a display panel displayed for the purposes of authenticating a super user;

Figure 7 is a display panel displayed to a super user for the purposes of configuring a user profile;

Figure 8 is a further display panel super imposed upon the display panel of Figure 7 for the purposes of effecting data access permissions for a specific partition during configuration of a user profile;

Figure 9 is a flow diagram showing the logical processes performed by a user invoking the PACU application;

Figure 10 shows a password entry box provided for authenticating a user to access the PACU application;

Figure 11 shows a partition access control table for the particular user authenticated to use the PACU application;

Figure 12 is a flow diagram showing the normal system operation incorporating the SDV and PACU application process flows; and

Figure 13 shows a user authentication box displayed to a typical user for authenticating the user to the SDV prior to booting of the operating system.

Best Mode for Carrying Out the Invention

The best mode for carrying out the invention will now be described with respect to several embodiments.

The first embodiment is directed towards a control system involving a partition access control utility (PACU) for allowing a user to change their data access control for various partitions of a data store to which they are permitted access in a computer system. In the present embodiment, the computer system is in the form of a standard personal computer (PC) comprising a central processing unit (CPU), standard peripheral devices such as monitor, keypad, mouse and printer, a data store in the form of a mass data medium such as a hard disk drive (HDD), and a security device (SDV) of the type described in patent specification WO 03/003242 for securing data access to the data store.

As described in patent specification WO 03/003242, the SDV is interposed in the data access channel between the CPU and the HDD, and controls data access to the HDD by users. This control is effected by using an authentication process, whereby a user permitted to access data on the HDD must be authenticated prior

to booting of the operating system of the PC and be provided with a specific partition access profile that determines the type of data access permitted to the various partitions of the data store of the PC. Furthermore, the SDV is designed to enforce the data access regime configured for a particular user authenticated by the system and deny access to the data store by users operating outside of the bounds of their configured profile, or by users that are not authenticated and/or spurious processes operating and attempting to access data outside of the bounds of the particular data access profile imposed upon the data store at a particular point in time.

As described, the authentication process is invoked during the operation of the basic input output system (BIOS) after the "drive ID" check is performed. Accordingly, the authentication program is run by the CPU on loading the "custom" boot sector provided by the SDV in place of the normal boot sector or master boot record normally stored in the data store.

As described, it is only after a user is properly authenticated and the processes undertaken by the user during operation of the authentication application program have been completed, that the BIOS program proceeds with permitting access to the data store and loading of the operating system under which the user may subsequently operate the computer and access the data store in accordance with their data access profile.

As shown in Figure 1, the SDV 11 is specifically designed to interact with the PACU 13, which is implemented as a software application and stored in a hidden location in the data store 15 of the PC that is not accessible to any users of the PC other than an administrator of the SDV itself.

In the present embodiment, the PACU application 13 is written as a Windows program developed in VC++ and MFC to operate within the Windows operating system 17. It interfaces with the Windows IDE device driver 19 via the Windows Application Program Interface (API) to communicate with the data store 21 along the IDE cable 23 of the data access channel. As illustrated, the SDV 11 is connected in line with the IDE cable 23 to intercept all communications provided

along the data access channel between the Windows IDE device driver 19 and the data store 21.

The PACU application uses services provided by the Windows API of the host operating system, which preferably is Windows 2000 or Windows XP, for communicating with the SDV and the user.

It should be appreciated that the PACU application can also be developed to interface with other operating systems such as LINUX and SUSI.

As shown in Figure 2 of the drawings, the PACU application 13 essentially comprises the logical processes of an authenticator 25 and a control system engine 27 to communicate database 29 that may constitute part of the SDV 11. The PACU application 13 is invoked to operate normally under the operation of the CPU 31 of the PC under the control of the operating system 17 and interacts with an SDV engine 35 of the SDV, that controls data access between the CPU 31 and the data store 15.

As previously described, the data store 15 may comprise a plurality of HDDs having a series of partitions, which in the present embodiment are C:, D:, E:, F:, G:, H: and I:, mapped across the data store formed thereby.

The control system engine 35 of the PACU application 13 further comprises a profile setter 37 and an editor 39, which are designed to configure the database 29 in a prescribed manner. These components will be described in more detail later.

The database 29 is designed to logically store two types of data access profile for each user permitted access to the data store 15 of the PC. These data access profiles include a master data access profile M1 to Mn for users 1 to n, and a current data access profile C1 to Cn. Each data access profile defines the data access permissions of a particular user for those partitions that the user is permitted access to.

For example, as illustrated in Figure 3 of the drawings, a user profile is shown where the user has access to six partitions indicated by the drives C:, E:, F:, G:, H: and I:, with the particular partition size indicated in the corresponding row of the adjacent partition size column. Further details indicating whether the partition is bootable, whether partition access control is enabled or disabled, and the current permissions applying to the particular partition or drive, are indicated in subsequent columns. As indicated in the last "current permissions" column, three data access permissions are available for each partition, namely; access, read/write access and no access.

The authenticator 25 of the PACU application 13 functions separately of the authentication program of the SDV 11 and is provided to authenticate users that are permitted to use the PACU. Thus, as will be described in more detail later, the SDV 11 is designed so that an administrator or super user of the SDV system is permitted to configure data access profiles of users who are permitted to access the data store 15 of the PC and can determine whether the PACU facility is available to a particular user or not.

The authenticator 25 works in conjunction with the control system engine 27 to interact with the database 29 via the SDV engine 35 to permit either super user access or normal user access of the PACU application with corresponding functionality applicable to the status of the user and their configured master data access profile.

As previously mentioned the data access profile stored within the database 29, includes the following:

- a user name and password for each permitted user,
- the partitions of the data store to which the user is permitted access, and
- the permissions state for each partition to which the user is permitted access.

The various permissions states are particularly characterised by providing different degrees of data access to the data stored within each partition, ranging from a low or no permission to read or write data from or to the partition, to a high or total permission to read or write data from or to the partition.

In the present embodiment, the range of permissions is as follows:

No access - no permission to read or write data.

Read Only - low permission generally consisting of no permission to write but high permission to read.

Read/Write - high or total permission to read and write data.

The profile setter 37 is particularly designed to allow setting of the master data access profile and the current data access profile of the user. The master data access profile effectively sets the scope within which a user may change or alter their current data access profile using the PACU application 13, if they are permitted access to same.

The editor 39 is designed for being invoked by either a super user or normal user of the PACU application 13 for editing the master data access profile or the current data access profile of a user, respectively. Thus, if a super user is identified by the authenticator 25 to the control system engine 27, the engine 27 allows the super user to operate the editor 39 in a manner so as to access and vary the master data access profiles of any permitted user of the computer, as stored within the database 29. On the other hand, if the authenticator 25 authenticates a user as a normal permitted user that has access to the PACU application 13, then the control system engine 27 permits the editor 39 to be invoked by the user in a manner so as to only allow changing of the current data access profile of that authenticated user and furthermore limit the editing that can be effected in respect of the current data access profile of the user to fall within the parameters determined by the master data access profile previously set for that particular permitted user.

In accordance with the present embodiment, the parameters that are determined by the master data access profile only permit changing the data access permission for a partition to the same or lower degree of data access than the data access permissions set in the master data access profile for that permitted user. Importantly, the determined parameters deny a user to change a data access permission for a particular partition to a higher degree of data access than specified for the permitted user in the master data access profile of that user.

By way of example, if a user only has "read only" access set for accessing partition or drive E: in their master data access profile, then that user can only change the current data access permission for that particular partition or drive to "no access", or back to "read only" access. They may not change the data access permission for that drive or partition to "read/write" access.

On the other hand, if "read/write" access was provided for that particular partition or drive in the master data access profile, then the user would have free range to change the current data access profile for this particular partition or drive to any of the aforementioned permissions, as desired.

However, in the case of the master data access profile for the particular partition or drive being set to no access, then that user would be denied from making any change to the current data access permissions for that partition or drive.

The profile setter 37 is invoked to control the editing of the current data access profile of a normal user so that a profile is not able to be set that does not conform with the parameters by the master data access profile for that user. Thus the profile setter 37 only permits a current data access profile of a user to be passed to the SDV engine 35 for subsequent use by the SDV 11 that conforms with the parameters of the master data access profile of the user and which is used to control data access of the user to or from the data store 15, under the operation of the CPU 31.

In order to obtain a better understanding of how the software of the PACU application 13 is designed for process flow and interaction with the user via a graphical user interface (GUI) provided as part of the Windows API, and indeed how the software would be implemented, regard will now be made to figures 4 to 13.

The software flow performed by the SDV 11 during the intialisation phase for setting up and configuring users of the PC and setting up PACU access is shown in Figure 4.

Installing the SDV hardware 11 by connecting it in line with the IDE cable 23 between the CPU 31 and the data store 15 is represented at 41. The HDD's of the data store 15 are then formatted with the required number of partitions at 43, followed by installing the HDD's under the control of the operating system of the computer at 45. A CD ROM containing the set up software for the SDV 11 is inserted into the CD ROM drive at 47 of the PC and the set up program loaded under the control of the operating system 17.

If the SDV 11 has not yet been initialised, the software flow at 49 invokes a process at 51 for setting up a super user for the SDV. The super user is able to set up user names and passwords for all permitted users of the PC and their master data access profiles. This process invokes a GUI at 53 to create a super user display panel 55, as shown in Figure 5 of the drawings. The process at 51 then interacts with the display panel 55 to allow a super user name to be created and a password to be set for the super user, using password confirmation, for subsequent authentication of the super user. The display panel 55 also allows the super user to enable PACU access for permitted users of the PC if desired and set a PACU password for the super user with confirmation of the PACU password and an identity string to authenticate the super user when invoking the PACU application 13. A "finish" button 57 is also provided at the bottom of the screen to allow the super user to exit the process at 59.

Once the super user account is created, the SDV 11 is considered to be initialised and progresses to a user account configuration state, where the super

user can set up individual user accounts for those users who are permitted access to the PC and to allow for their authentication.

As shown, the software flow may proceed to commencing super user configuration of user accounts commencing at step 61 either immediately after setup of the super user via the exit process 59, or via the decision box 49 if the SDV has previously been initialised. The process commences at 61 by displaying a user authentication panel 63, as shown at Figure 6 of the drawings, and prompting the super user to enter their user name and pass phrase for correct authentication at 65. An authentication button 67 is provided on the display panel 63 to effect authentication at 69. If a super user is not authenticated at this stage, the program flow exits at 71 and the setup program for the SDV 11 needs to be restarted and the process repeated until such time as a super user is authenticated.

On valid authentication at 69, the software invokes a process at 73 that allows a super user to create each individual user account, assigning individual user pass phrases and access rights to configure the master data access profile for the individual user.

This process involves a display panel 75 being displayed by the GUI for the super user to configure each individual user profile at 77, as shown in Figure 7 of the drawings. The display panel 75 includes data entry fields for the user name, password, password confirmation, PACU password (if the PACU facility is enabled), PACU password confirmation and the identity string of the individual user, at successive rows of the display panel 75. The display panel 75 also includes two partition panels, the first 79 listing the various partitions formatted on the HDD of the data store 23. The second partition panel 81 provides for the display of those partitions that are selected for access by the super user for the particular user.

As shown in Figure 7 of the drawings, the partition name and memory address map is provided for each formatted and selected partition. The "save" button 83 and the "return to main menu" button 85 are provided at the bottom of the display

panel 75 to save the configuration and return to normal program flow, respectively.

In order to select partition access, permissions and PACU accessibility for individual users, the process 87 is invoked which involves the GUI displaying a display panel 89 super imposed on the user profile configuration panel 77, as shown in Figure 8 of the drawings.

The display panel 89 allows the start sector address for the particular partition access of the user to be identified, the partition size, access mode and setting of the PACU mode, in successive rows. As indicated, drop down menus are provided for the "access mode" and the "PACU mode" entry fields to provide selection from fixed permission access modes, i.e. read only, read/write and no access, for the purposes of setting the access mode, and "enabling" or "disabling" flags for the PACU access mode, respectively. An "ok" button 93 and a "cancel" button 95 are provided at the bottom of the display panel 91 to allow for completion of the partition details selection of the highlighted partition.

After each user profile configuration has been completed, the software flow proceeds to checking whether the super user has configured all users at 97, and if not, initiating the user profile configuration at 73 for another user, or exiting the initialisation procedure at 99 after the super user has indicated that all users have been configured.

As previously described, the PACU 13 operates as an application under the operating system 17, interfacing with the Windows API to communicate with a user and the SDV engine 35. The software flow of the PACU 13 is shown in Figure 9 of the drawings. Prerequisites for PACU operation are:

(i) installation and configuration of the SDV 11,

(ii) invoking of PACU by a previously authenticated user via the SDV, and

(iii) compatibility of PACU with the operating system under which the PACU application is operating.

The PACU application is invoked by a user at 101 and proceeds at 103 to display a password entry display panel 105 as shown in Figure 10 of the drawings at 107. The display panel invites the user to enter their PACU password for authentication, using the password configured for the user by the super user as previously described.

The display panel 105 includes a "login" button 107 and an "exit" button 109 to continue or exit the PACU authentication process. If continued, by pressing the "login" button 107, the PACU application proceeds with communicating with the SDV 11 for authentication at 111, whereupon varification of the authentication occurs at 113. If the user is not authenticated, the process returns to asking the user to enter their PACU password at 103 once more. If the user is authenticated, then the process continues with the PACU control system engine 27 retrieving the partition access control information from the SDV 11 at 115.

The partition access control information for the authenticated user is displayed in a table 117 via the GUI at 119. This table 117 corresponds to that described previously at Figure 3 of the drawings, whereby only those partitions to which the user has been allocated access by the super user are displayed in successive rows. The user is provided with the option to modify those permissions within this table to the extent permitted by the profile setter 37, where the degree of data access can be reduced or reasserted under the "current permissions" column. This is effected by clicking on the particular entry of the "current permissions", whereupon a drop down menu is presented providing the available permissions that are selectable for the particular drive, within the bounds of control determined by the master data access profile previously set for the permitted user by the super user.

An "apply" button 121 and a "close" button 123 are provided at the base of the display panel 117 so that software flow may be progressed at 125. Moreover, if a user has not modified any partition access control and the "close" button 123 is

asserted, then the PACU program is exited directly at 127. On the other hand, if the user has modified the current permissions and applied them by asserting the "applied" button 121, then the profile setter 37 sends new partition access control information to the SDV 11 at 129 to set the permitted users current data access profile separate from the master data access profile, as stored in the database 29.

Thereupon, the PACU application is exited once more at 127.

The integration of the normal software flow of the PACU application, in conjunction with normal SDV system operation, is shown at Figure 12 of the drawings. In this drawing, the corresponding process steps to those described in conjunction with PACU flow control above have been identified using the same reference numerals to facilitate understanding of this perspective of the operation of the control system.

During normal operation of the SDV 11 and the PACU application 13, the computer is powered up at 131 and the computer BIOS invoked which subsequently loads the start-up code from the SDV boot device at 133.

The user is prompted at 135 to enter their name and pass phrase via the user authentication display panel 137, which is displayed to the user by the GUI at 139. On pressing the "authenticate" button 141 provided at the bottom of the display panel 137, the SDV authentication process is invoked to authenticate whether the user is a permitted user of the computer system setup by the super user of the SDV, as previously described.

If the user is not authenticated at 143, then an attempt counter is incremented (or decremented) and the permitted number of authentication attempts checked at 145. If the number of permitted authentication attempts are exceeded, the software process is exited at 147 and the computer system shutdown, as a consequence of the user failing to authenticate themselves. On the other hand, if the number of permitted attempts to authenticate the user have not yet been reached, then the software flow returns to prompting the user to enter their name

and pass phase at 135 to provide the user with another attempt to authenticate themselves.

On authentication of the user at 143, the SDV 11 decrypts the valid user partition access information, which in the present embodiment is stored on the database 29 in a hidden area of memory at 149, to control subsequent data access to the data store in accordance with the current user profile configured for the permitted user.

The computer operating system 17 is then started at 151, whereupon the SDV 11 checks all subsequent data access attempts to the data store 15 at 153, in accordance with the current data access profile of the permitted user. If a data access attempt at 155 is not in accordance with the current data access profile of the user, then the data transfer process, being either a "read" or "write" is blocked at 157, without any access to the HDD being effected. On this, the SDV 11 returns to its data checking state at 153.

If, on the other hand data, access is in conformity with the current data access profile of the user at 155, then the data is checked to ascertain wether the PACU application is being invoked at 159. If not, data access to the HDD of the data store 15 is continued at 161, and the power down condition checked at 163. If the power down condition is asserted at 163, the software flow is exited at 165 and the power down process effected by the computer system. If the power down condition is not asserted, then the software flow returns to the SDV 11 checking data access attempts at 151, once again.

If at 159 the SDV 11 determines that the PACU application 13 is invoked, then the PACU software flow process as described with respect to Figure 9 is progressed. Accordingly, the user is prompted to enter the PACU password at 103 and the PACU authentication display panel 105 is displayed to the user by the GUI at 107. The PACU authentication process proceeds and a determination as to whether the user has valid PACU access or not determined at 113.

If so, the PACU application 13 reads the partition access control information stored in the database 29 at 115, and displays the current data access profile of the user at 119.

If the user has modified its access rights at 125 using the editor 39 then the PACU application updates the current data access rights stored in the database 29 of the SDV, using the profile setter 37 at 129, and proceeds to exit the PACU application 13 at 127. Alternatively, if access rights are not modified at 125, then the PACU application exits at 127 directly. On exiting the PACU application 13, the power down condition is again checked at 163, and if asserted, the program flow is exited at 165. If not asserted, the software flow returns to the SDV 11 checking data access attempts at 153 once more.

The second embodiment is exactly the same as the preceding embodiment except that the SDV 11 is incorporated into the design of a bus bridge circuit, either provided in the south bridge of the mother board on the CPU side of the computer system, or alternatively, in the bridge circuit provided on the data store side, in the case of using a serial AT attachment (SATA) standard for communicating with the data store, as described in the applicant's international patent specification accompanying its International Application PCT/AU2004/000210.

It should be appreciated that the control system described in either of the embodiments of the best mode allows a single authenticated user to change the read and write access control partitions for which that person has authorisation, during normal system operation under the operating system, as opposed to changing the user profile during the pre-boot process of the SDV. Thus, the PACU application is installed as standard application software on the hard disk of the computer system and runs under the control of the PC's normal operating system, albeit under the super control of the SDV.

In this manner, the system administrator or super user need create only one master data access profile for each user configuring the data access permissions for each partition accessible to the user and enabling PACU access to each user

and the partitions accessible thereto. This means that the system super user still has complete control over the data access that is allowed for the partitions by a permitted user, but allows each permitted user having PACU access the facility of altering their own profile within prescribed parameters determined by the master data access profile, as originally configured by the super user for that permitted user.

For example, in Table 2 below, user 1 authenticates once at start-up. The user may then change the read/write access to the D:, E: and F: partitions at any time using the PACU application. Access to the C: and G: partitions are set by the administrator/super user and cannot be changed. For user 2, the partition access has been set by the administrator and cannot be changed. Running the PACU application by user 2 will have no effect on the system operation.

User: 1	Profile: 1	Disk Access	C:Read/Write
			D: PacSoft Control
			E: PacSoft Control
			F: PacSoft Control
			G: Read Only
User: 2	Profile: 1	Disk Access	C: Read/Write
			H: Read/Wrtie

Table 2

Some of the advantages provided by the present invention in allowing partition access control to a permitted user within limits as determined by the system administrator or super user are as follows:

- The system administrator has complete control as to which users and what partitions may be controlled by the PACU application.

- The user requires only one profile for authentication at start-up.
- The number of passwords a user must remember are reduced compared to one user having many different access profiles.
- The user may alter read or write access permissions for those partitions within their permitted bounds of control at any time during normal system operation in order to protect data on the data store.
- The user may disable access to all partitions allowing them to leave the computer in a secure state, without turning the power off. A third party must know the permitted users password to be able to gain access to the disabled partitions.
- The user authentication process at start-up is unchanged. No potential security weaknesses are introduced by adding the additional functionality.
- The PACU application has minimal impact on the operation security features of the SDV provided on a computer system. The existing mode of operation where the user must power down the computer to switch profiles in a highly secure application is still supported.
- The SDV is still independent of the operating system. Only the GUI utility must be made to run with different operating systems.
- The PACU application can be distributed on CD or downloaded from a website provided on the Internet.
- The PACU application can be stored in an encrypted "read only" partition on the HDD to help maintain system integrity.
- The PACU application functionality can be changed at any without the need to create new user partitions or to change the SDV hardware.

- The PACU application has utility as a remote administration tool.
- The simplicity of operation of the PACU application permits it to be easily identified as a software utility that does not directly affect the security provided by the SDV.

It should be appreciated that the present invention is not limited to the best mode and the specific embodiments described herein. Accordingly, alternative embodiments and variations from the best mode may be envisaged in accordance with conventional software and computer engineering practice, without departing from the spirit nor scope of the present invention.

Dated this 5th day of March 2004.

Secure Systems Limited

Wray & Associates
Perth, Western Australia
Patent Attorneys for the Applicant(s)

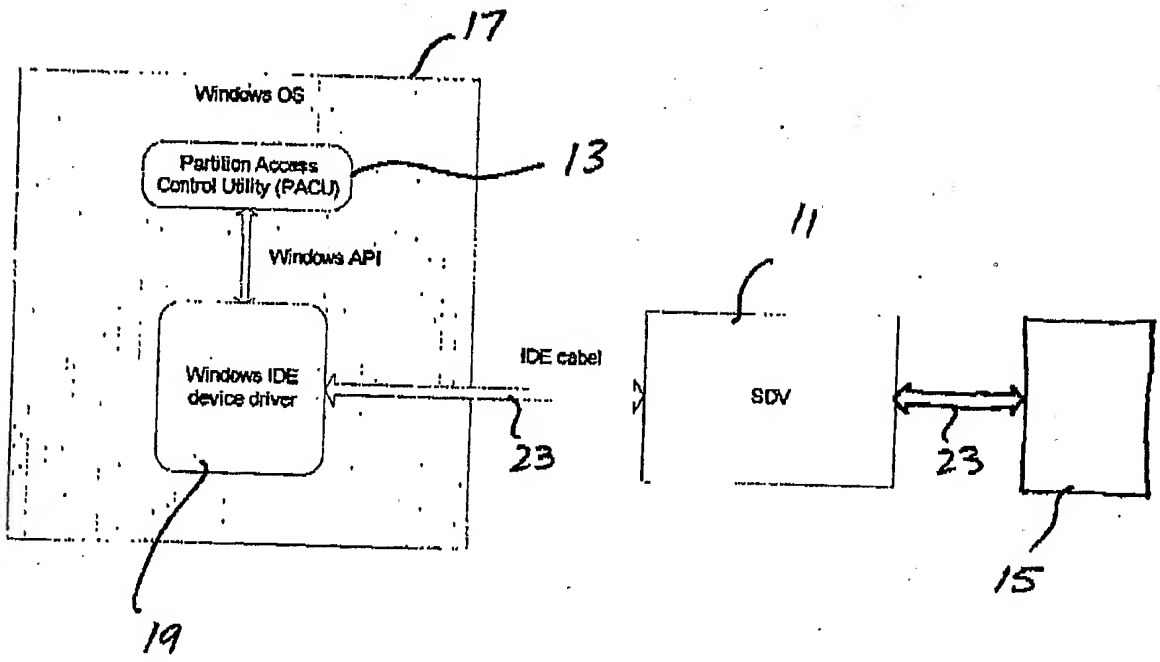
17
Windows OS
Partition Access Control Utility (PACU)
13
Windows API
Windows IDE device driver
IDE cabel
23
19
11
SDV
23
15

Fig 1

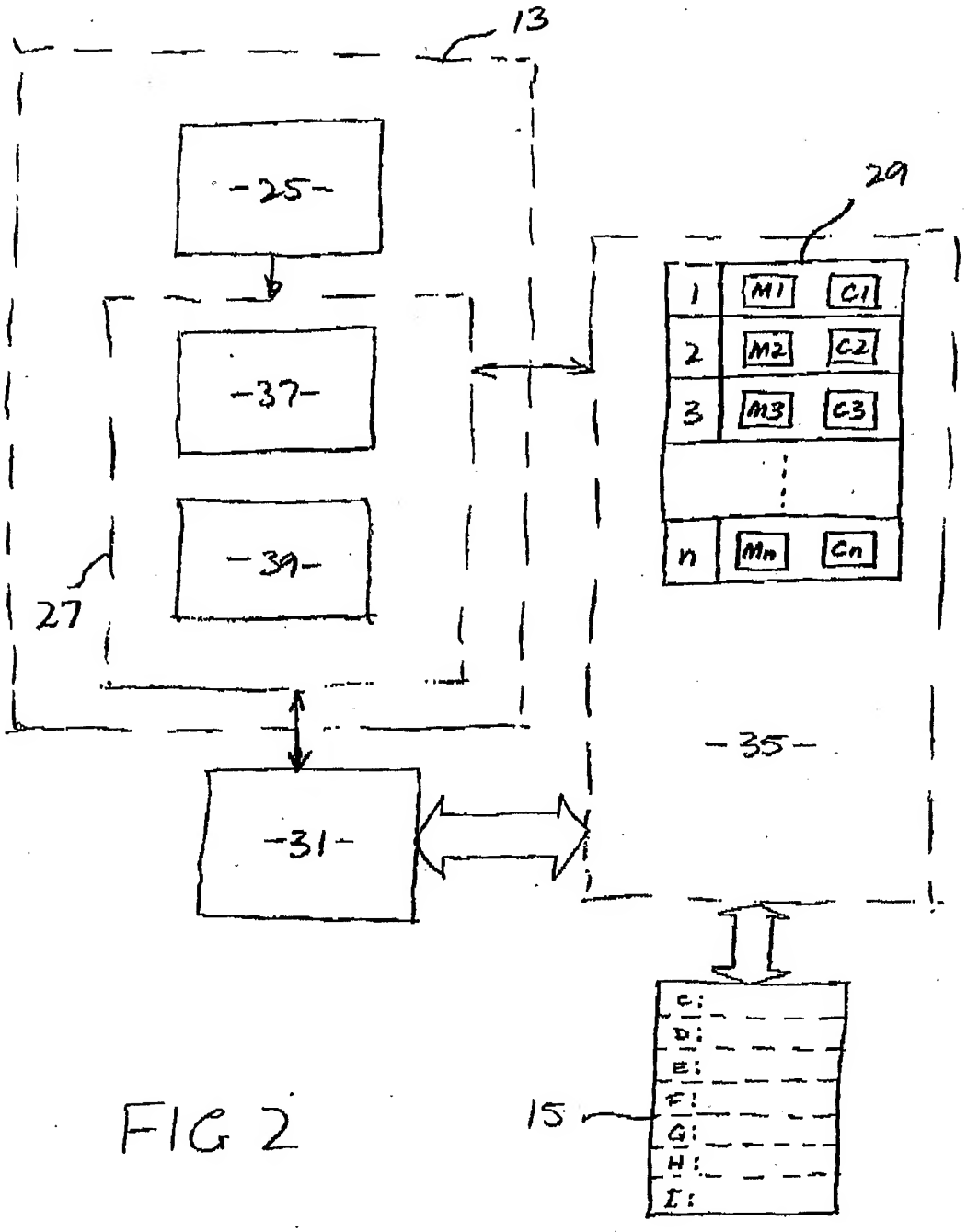

FIG 2

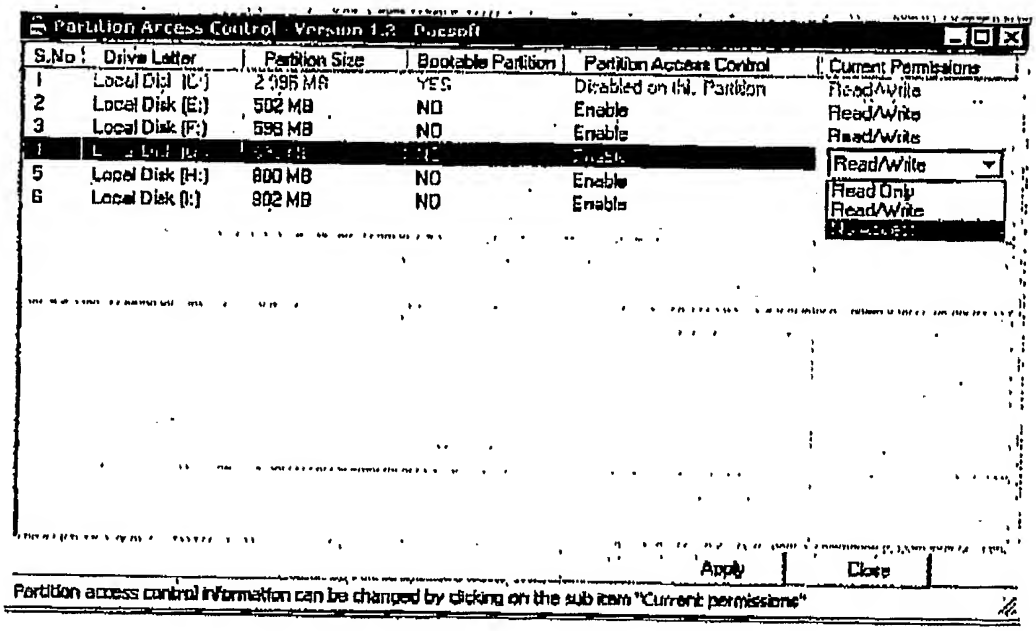
Partition Access Control - Version 1.2
S.No
Drive Letter
Partition Size
Bootable Partition
Partition Access Control
Current Permissions
1 Local Disk (C:) 2 995 MB YES Disabled on thi. Partition Read/Write
2 Local Disk (E:) 502 MB NO Enable Read/Write
3 Local Disk (F:) 598 MB NO Enable Read/Write
5 Local Disk (H:) 800 MB NO Enable
6 Local Disk (I:) 902 MB NO Enable
Read/Write
Read Only
Read/Write
Apply
Close
Partition access control information can be changed by clicking on the sub item "Current permissions"

Fig 3

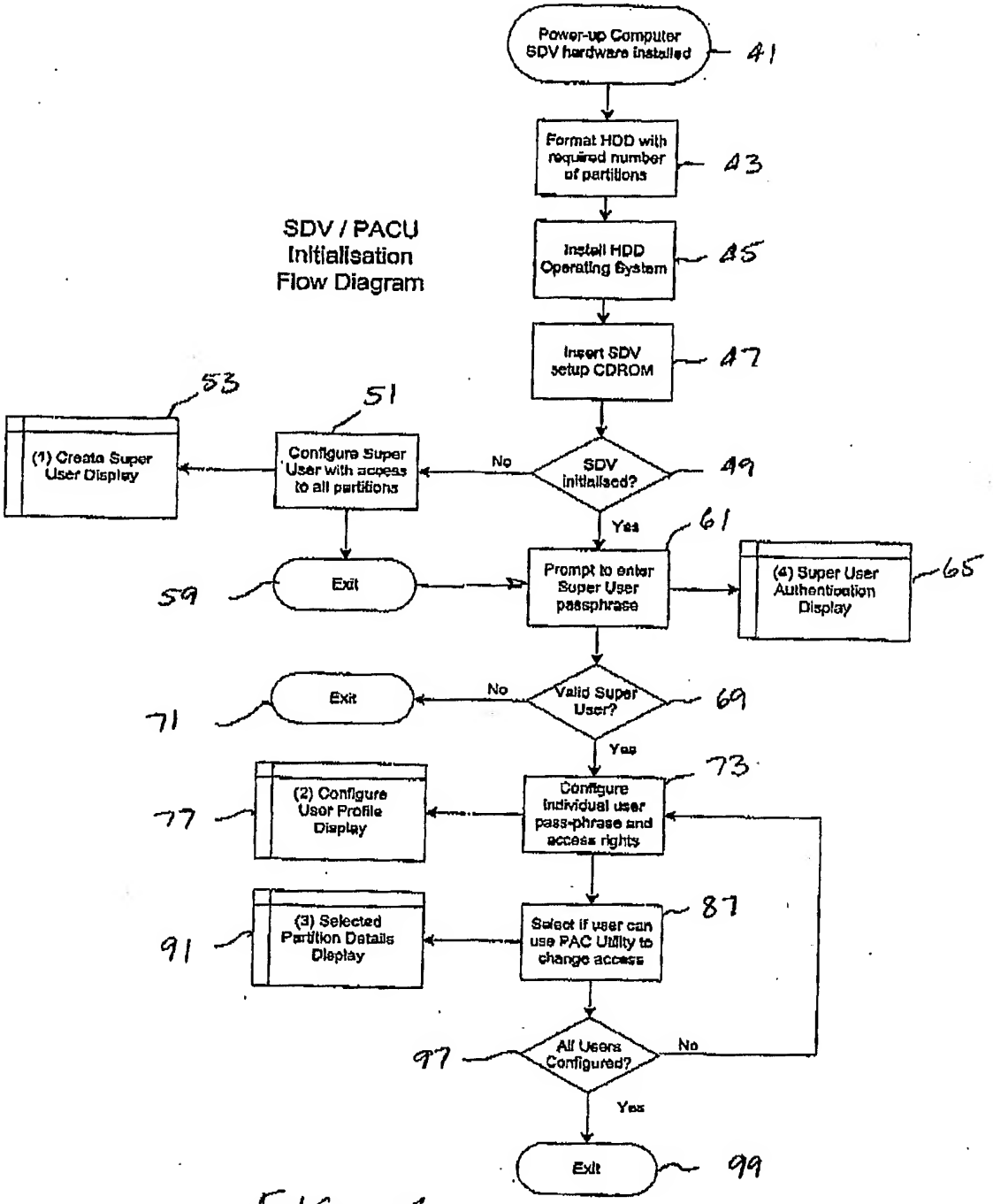
SDV / PACU
Initialisation
Flow Diagram
Power-up Computer SDV hardware installed
41
Format HDD with required number of partitions
43
Install HDD Operating System
45
Insert SDV setup CDROM
47
SDV initialised?
49
No
Yes
Configure Super User with access to all partitions
51
(1) Create Super User Display
53
Exit
59
Prompt to enter Super User passphrase
61
(4) Super User Authentication Display
65
Valid Super User?
69
No
Exit
71
Yes
Configure individual user pass-phrase and access rights
73
(2) Configure User Profile Display
77
Select if user can use PAC Utility to change access
87
(3) Selected Partition Details Display
91
All Users Configured?
97
No
Yes
Exit
99

FIG 4

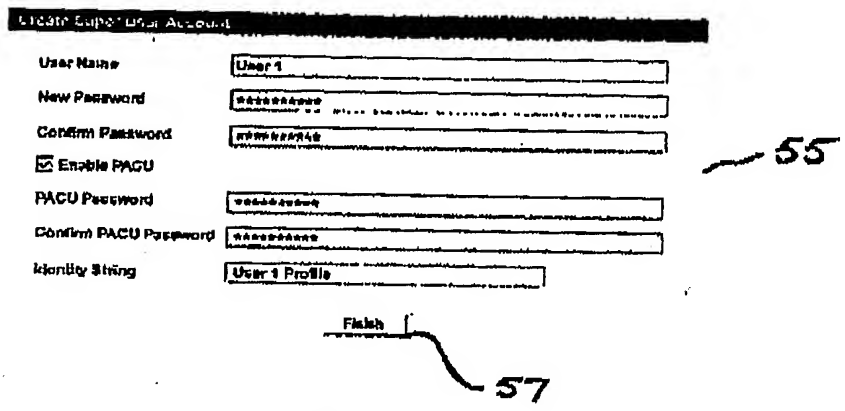
User Name
User 1
New Password
Confirm Password
Enable PACU
PACU Password
Confirm PACU Password
Identity String
User 1 Profile
Finish
55
57

Fig 5

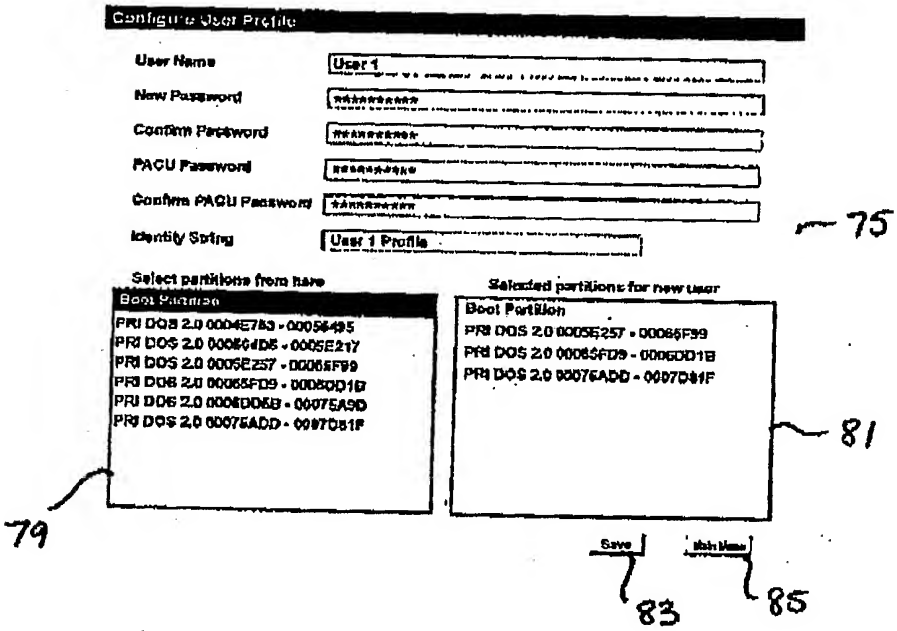
User Name
User 1
New Password
Confirm Password
PACU Password
Confirm PACU Password
Identity String
User 1 Profile
75
Select partitions from here
Boot Partition
PRI DOS 2.0 0004E783 - 00056495
PRI DOS 2.0 00056dD5 - 0005E217
PRI DOS 2.0 0005E257 - 00065F99
PRI DOS 2.0 00065FD9 - 00060D1B
PRI DOS 2.0 00060D5B - 00075A9D
PRI DOS 2.0 00075ADD - 0007D81F
Selected partitions for new user
Boot Partition
PRI DOS 2.0 0005E257 - 00065F99
PRI DOS 2.0 00065FD9 - 00060D1B
PRI DOS 2.0 00076ADD - 0007D81F
81
79
Save
83
85

Fig 7

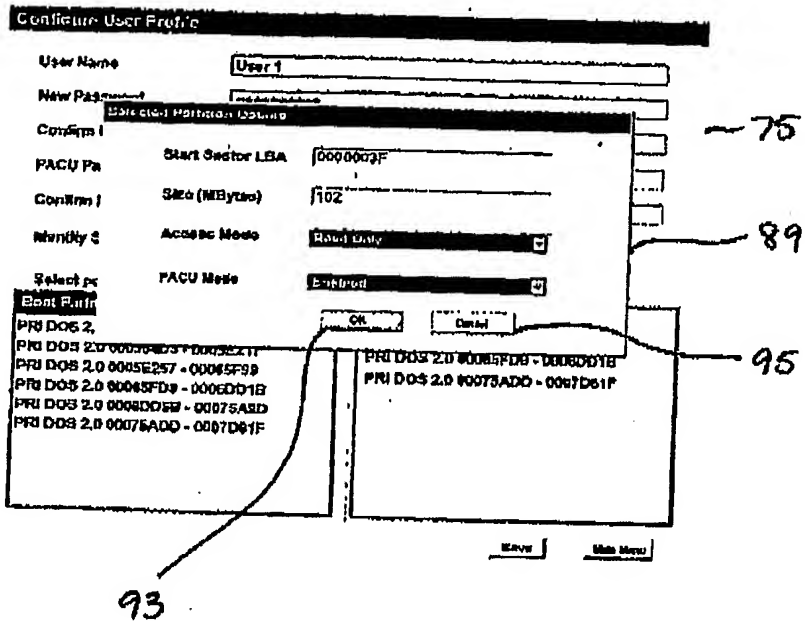
User Name
User 1
Start Sector LBA
00000003F
Size (MBytes)
102
Access Mode
PACU Mode
OK
PRI DOS 2.0 00065FD9 - 0006DD1B
PRI DOS 2.0 00073ADD - 0007D61F
75
89
95
93

Fig 8

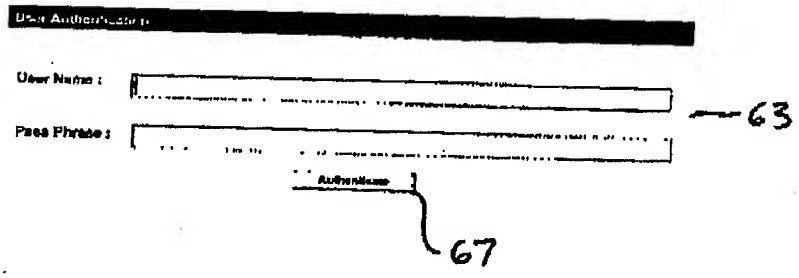
User Name :
Pass Phrase :
63
67

Fig 6

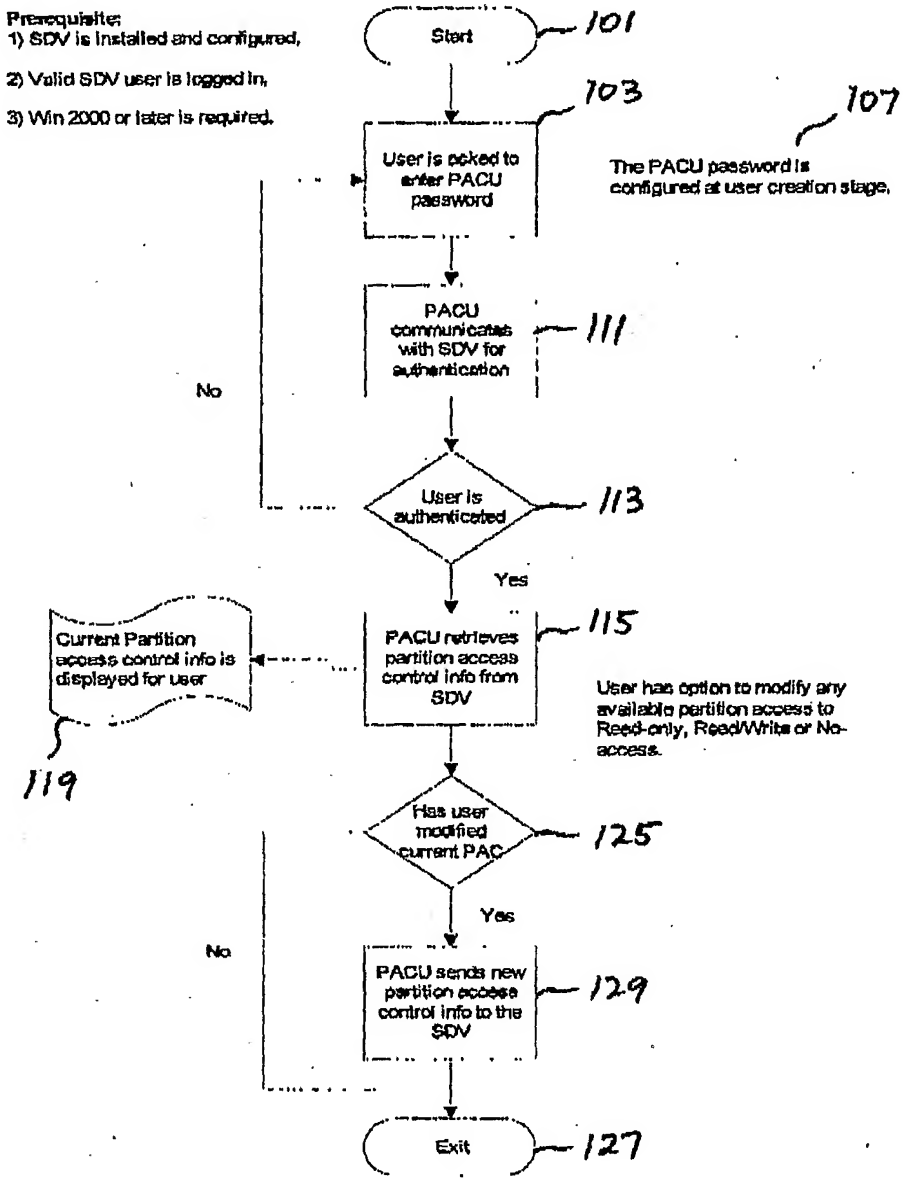
Prerequisite:
1) SDV is installed and configured,
2) Valid SDV user is logged in,
3) Win 2000 or later is required.
Start
101
User is acked to enter PACU password
103
107
The PACU password is configured at user creation stage.
PACU communicates with SDV for authentication
111
No
User is authenticated
113
Yes
Current Partition access control info is displayed for user
119
PACU retrieves partition access control info from SDV
115
User has option to modify any available partition access to Read-only, Read/Write or No-access.
Has user modified current PAC
125
Yes
No
PACU sends new partition access control info to the SDV
129
Exit
127

Fig 9

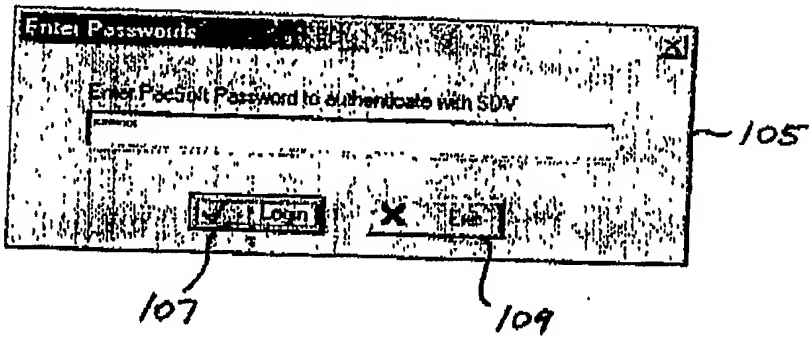

Fig 10

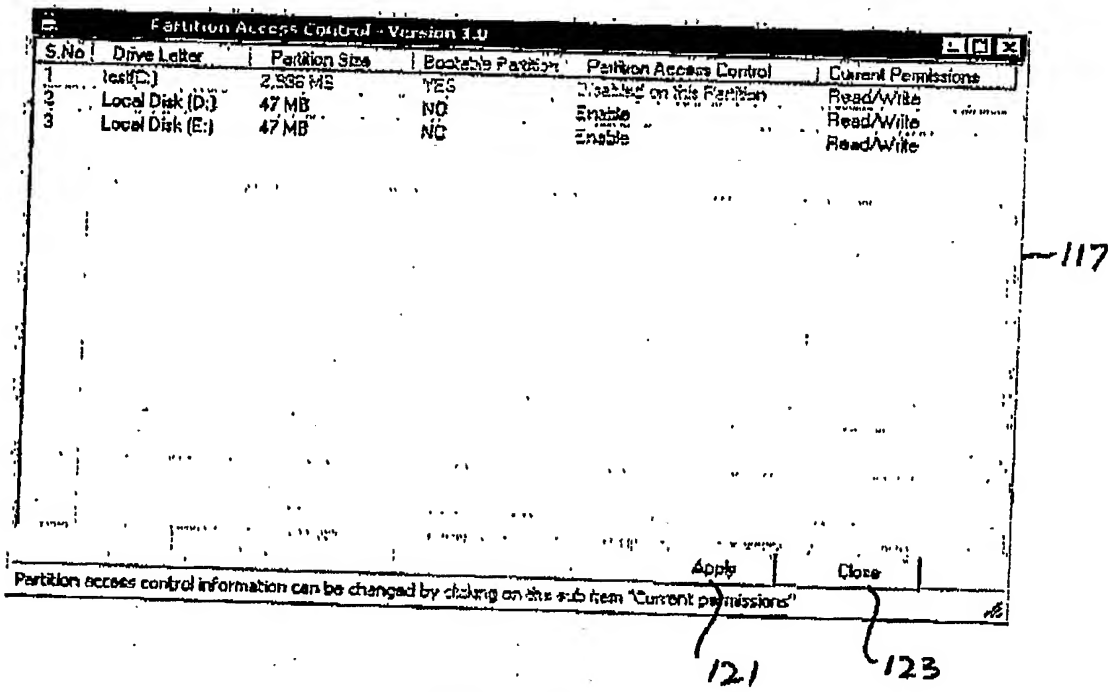

Fig 11

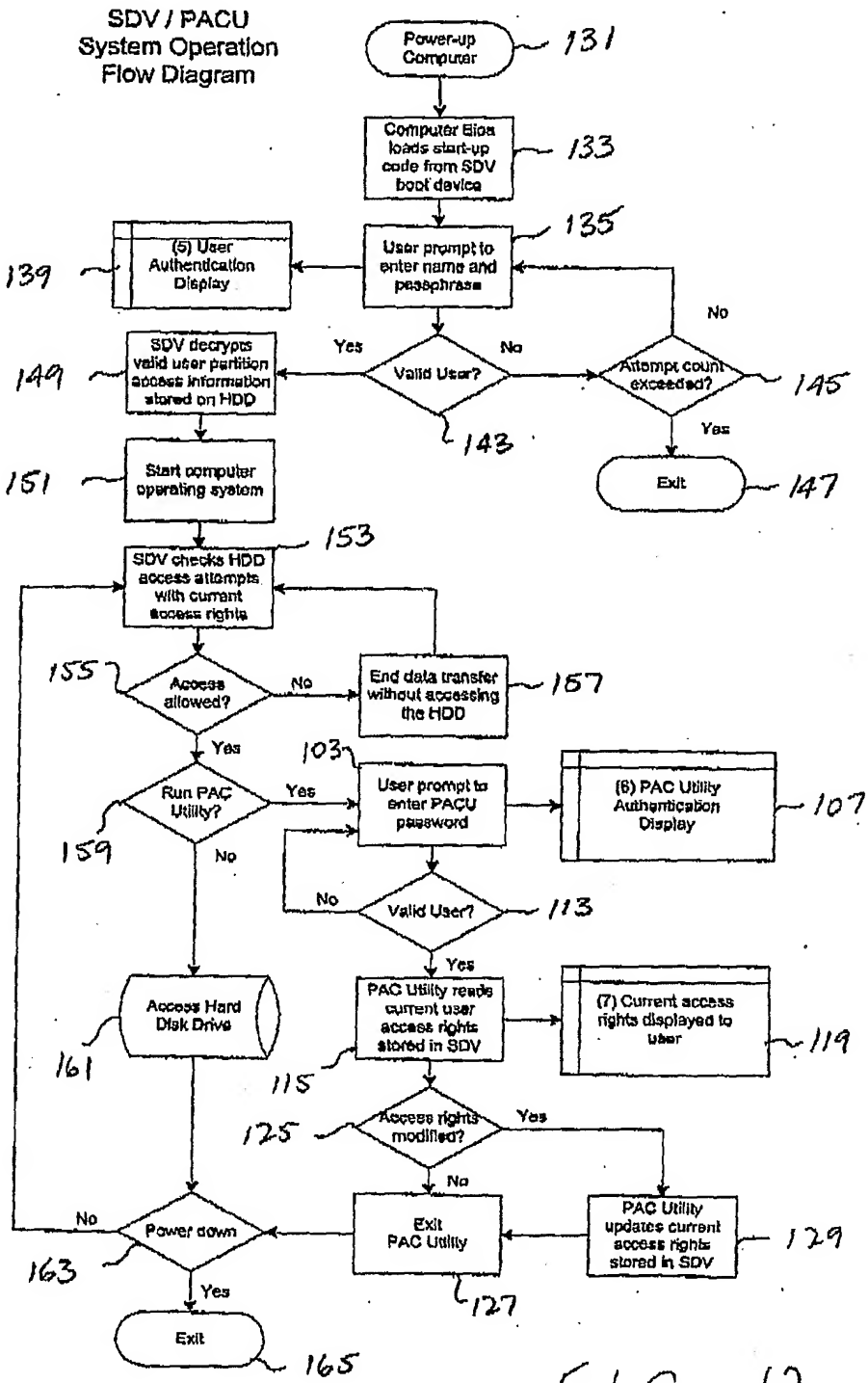
SDV / PACU
System Operation
Flow Diagram
Power-up Computer
131
Computer Bios loads start-up code from SDV boot device
133
User prompt to enter name and passphrase
135
(5) User Authentication Display
139
Valid User?
143
Yes
No
Attempt count exceeded?
145
No
Yes
Exit
147
SDV decrypts valid user partition access information stored on HDD
149
Start computer operating system
151
SDV checks HDD access attempts with current access rights
153
Access allowed?
155
No
End data transfer without accessing the HDD
157
Yes
Run PAC Utility?
159
Yes
No
103
User prompt to enter PACU password
(6) PAC Utility Authentication Display
107
No
Valid User?
113
Yes
Access Hard Disk Drive
161
PAC Utility reads current user access rights stored in SDV
115
(7) Current access rights displayed to user
119
Access rights modified?
125
Yes
No
No
Power down
163
Yes
Exit PAC Utility
127
PAC Utility updates current access rights stored in SDV
129
Exit
165

FIG 12

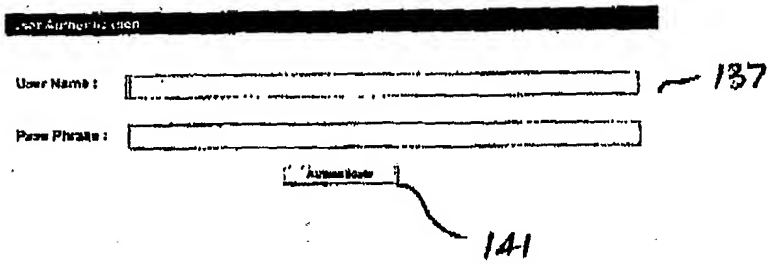

Fig 13